Cracking the Windows 95 Screen Saver Password
Article Extracted from 2600 Magazine
Volume 13 #4
==========

Defeating the Windows 95 Screensaver
by rdpzza

While many may consider this a trivial exercise, cracking the password scheme for Win95 may be useful to some of you out there. Some may even find ways to have phun with it as well.

To start with, you need to know where to look. In 3.1, the password was kept in

the control.ini. Although 95 also uses the control.ini, it does not use it for keeping the password information. Foe 95, you will have to look in each of the user.dat files. I say each because if you have multiple users, each user may have a profile saved on the hard drive. The default user.dat file is in the \windows directory. The other user.dat files can be found in the directory \profiles\username where username changes. As you may know, user.dat is one of the two files used for the registry and its is very important. User.dat will carry the attributes "shr" so you will have to look accordingly. Also, since it is so important, a backup is kept, namely user.da0. This may be the previous user.dat, say when the user changed passwords...

Anyway, now that you have the file, where is it? If you scan the file for passowrd, you will come up with the setting of whether or not the screen saver is password protected. This may be enough for you so you can just change it and be done. While this little change will be noticed, it will get you by the password. If, however, you wish to actually find out the what the pass phrase is, read on.

Why find out what the pass phrase is, you ask? Because a lot of times users are stupid, lazy, have bad memory or any combination of these and reuse passwords or schemes any time a key is needed. This is especially true in network environments and even more so when 95 is used as the workstation OS. In such systems, there is the possibility of changing the logon password and the screen saver password at the same time. I wonder how that can be useful?

Back to finding out what the phrase is. 95 has been rumored to use dual case. Let me clear this rumor. It does not. It uses the "all upper" coding for the password like 3.1. The maximum length of the screen saver password is 14 characters long. It will allow you to enter longer passwords, but 95 will act screwy; it won't require the password from screen saver, it will hang, etc.

OK, so we have the file. Look for the string "ScreenSaver_Data". After this is an even string of numbres and letters ending in 00. THere is the encrypted pass phrase. The pass phrase is different from 3.1 in that 95 uses what I call "encrypted-couplets" meaning that for every character in the phrase, there are two encryption values. The

first
encrypted couplet (EC) is the first hex digit of the unencrypted ascii value, and the second
EC is the second hex digit. For example, say the first two hex digits after the string
"ScreenSaver_Data" are 31 41 (1A in ASCII). The 31 represents (after decryption) 5 and
the 41, 2. Put the digits together and you have 52h, R in ASCII. Keep this concept in
mind while decoding the EC's because the decryption scheme is the same for each value, only
the key changes.

Example of Screen Saver EC's decoded to password.

1AAAA26473D28 <- code in the user.dat
RDPZZA <- Win95 SS password

Try it out.

Text file downloaded from the HackerZ Hideout @ www.hackersclub.com/km